From: **Mark Chaplin**
Date: Tue, Apr 11, 2017 at 6:34 AM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

This submission is provided by the Information Security Forum (ISF), which is an independent, not-for-profit organisation specialising in cyber security and information risk management. We have reviewed the draft update of the ***Framework for Improving Critical Infrastructure Cybersecurity*** and submit the following comments.

The comments are based on feedback obtained within the ISF Membership (400+ global organisations), often from Member organisations that use the ISF's Standard of Good Practice for Information Security (ISF Standard) to manage information risk and cyber risk. These include ISF Members that:

- are based in the United States as well as other regions across the world
- use the Cybersecurity Framework either as a reference or as the basis for improving cyber security in their organisation
- are familiar with or have an interest in the Cybersecurity Framework.

We have engaged with Members in a broad range of different industry sectors (including banking, insurance, technology, manufacturing, transportation and energy) regarding the NIST Cybersecurity Framework (CSF), using our web-based portal, Chapter meetings and through both face-to-face and telephone conversations.

The most common request expressed by organisations across the ISF Membership is for the inclusion, in the Cybersecurity Framework Core (Appendix A), of references to the ISF's Standard of Good Practice for Information Security. ISF Members explain that inclusion of these references will provide a range of benefits, including help:

- promote the importance of these standards/frameworks to senior executives
- achieve greater alignment between these and other standards/frameworks
- support broader cyber security assessment and benchmarking activities
- identify the most important or effective cyber security controls and arrangements
- demonstrate greater levels of cyber security assurance to senior executives and other key stakeholders.

The comments provided in this email are grouped according NIST's Request For Comments questions.

Are there any topics not addressed in the draft Framework Version 1.1 that could be addressed in the final?
While the NISF CSF does not provide detailed coverage of cyber security-related topics, comparison against the ISF Standard has highlighted possible gaps in the Framework that NIST should consider. These gaps, grouped according to the 17 categories in the ISF Standard, include cyber security practices or disciplines covering:

1. **Security (Cybersecurity) Governance**, particularly relating to establishing and maintaining a security governance framework, which includes setting direction (for cybersecurity) and performing security assurance activities.
2. **Information (Cyber) Risk Assessment**, particularly relating to determining the requirements for protecting the confidentiality, integrity and availability of information, and assessing non-technical vulnerabilities.
3. **Security Management**, particularly relating to establishing an information security (cybersecurity) function and running information security (cybersecurity) projects.
4. **People Management**, particularly relating to managing the complete employment life cycle (for all stakeholders.
5. **Information Management**, particularly relating to document management and protecting information in physical form.
6. **Physical Asset Management**, particularly relating to managing the complete hardware life cycle, protecting office equipment (such as telephones, conferencing facilities and printers), protecting mobile technology (including employee-owned devices).
7. **System Development**, particularly relating to software acquisition, system design/build, security testing, quality assurance, system promotion and post-implementation review.
8. **Business Application Management**, particularly relating to the configuration and protection business applications (including browser-based applications and spreadsheet-based applications) and performing information validation.
9. **System Access**, particularly relating to user authorisation (i.e. the process before granting access), access control mechanisms (covering password, token and biometric), the sign-on process and managing customer connections and access arrangements (including contracts).
10. **System Management**, particularly relating to technology components such as virtual servers and network storage systems, and related service level agreements.
11. **Networks and Communications**, particularly relating to network device configuration (including wireless and firewalls), protecting physical and VoIP networks, managing external network connections, and protecting commonly used technology such as email, instant messaging, telephony and conferencing equipment.
12. **Supply Chain**, particularly relating to the use of outsourcing and cloud computing, and managing cloud service contracts (and equivalent).
13. **Technical Security Management**, particularly relating to security architecture (including the adoption of security architecture principles), identity and access management (including federated), digital rights management, and managing cryptographic technology and solutions (including public key infrastructure).
14. **Threat and Incident Management**, particularly relating to providing cyber attack protection (i.e. comprehensive protection against the complete cyber attack chain) and providing emergency fixes.
15. **Local Environment Management**, particularly relating to coordinating security activities, and protecting against hazards (including power supply protection).

16. **Business Continuity**, particularly relating to business continuity strategy, establishing resilient technical environments, planning business continuity, establishing business continuity arrangements and performing business continuity testing.

17. **Security Monitoring and Improvement**, particularly relating to security audit planning, fieldwork (including penetration testing), reporting and monitoring, performing security monitoring and undertaking information security compliance activities.

How do the changes made in the draft Version 1.1 impact the cybersecurity ecosystem?
The inclusion of the topic on supply chain is important and will be welcomed by organisations. I would encourage consideration beyond technology (hardware and software) to include managing the risks associated with engaging with organisations in the supply chain (upstream and downstream).
The introduction of the measurement section is also important as organisations need to establish and maintain a mechanism that supports ongoing cyber security assurance to stakeholders including senior executives.
Consistency of content could be improved across different sections. For example, the descriptions of each Tier vary, which can make it difficult for some readers to understand the elements between them that make a difference and to determine how to progress from one Tier to the next.
Examples of what a completed Profile looks like would be useful for many readers.
Diagrams could be more informative to help the reader understand the concepts conveyed in the body text. For example, the layout of Framework Core could include labelling the rows and columns would be useful.

For those not currently using Version 1.0, does the draft Version 1.1 affect your decision to use the Framework? If so, how?
Organisations not currently using Version 1.0 would probably benefit from a greater focus and more guidance on understanding, identifying, measuring and managing cyber risk, particularly in the context of the organisation's approach to information risk and operational risk. This will help security practitioners interpret Tiers, define Profiles and use the Framework Core more effectively.

Does this proposed update adequately reflect advances made in the Roadmap areas?
Sharing of cyber risk-related information is a strong theme in Version 1.0 and this draft (1.1). The extensive coverage of cyber security-related topics in the ISF Standard means inclusion of references in the Framework Core will strongly support the alignment requirements.

Is there a better label than "version 1.1" for this update?
The volume and type of changes proposed warrant the version 1.1 (i.e. not 2.0). Depending on the future review cycle applying the date to the title of the document might be useful.

Based on this update, activities in Roadmap areas, and activities in the cybersecurity ecosystem, are there additional areas that should be added to the Roadmap? Are there any areas that should be removed from the Roadmap?
As documented above, a focus on managing cyber risks would be beneficial to many organisations. This should include:

- an overarching risk management framework that aligns cyber, information and operational risk

- a risk assessment methodology that encourages a rigorous and scientific approach to scoping assessments, determining business impacts, profiling threats, assessing vulnerabilities, evaluating risks and treating them according to the organisation's risk appetite
- an ongoing risk management improvement programme, supported by defined metrics, reporting using defined KRIs and providing assurance of cyber protection in place.

Conclusion

Through the ISF's unique operating model we can provide NIST with expertise and best practice from our extensive research programme, our comprehensive portfolio of risk management tools and our Member engagement events.

As the ISF's primary contact for the National Institute of Standards and Technology, I will be participating in the forthcoming Cybersecurity Framework Workshop in May. During this workshop I will contribute to the development of the Framework, based on the ISF's experience working with more than 400 leading global organisations. In the meantime, if there are any questions please contact me. I can be reached by email and by telephone.

Regards
Mark

Note on the ISF Standard and Research Programme

The ISF Standard provides complete coverage of the NIST CSF, as well as other standards, including ISO/IEC 27002, COBIT 5 for Information Security, PCI DSS, CIS Critical Security Controls and ASD Strategies to Mitigate Cyber Security Incidents. The ISF Standard is supported by comprehensive cross-references to the current NIST CSF Core, which is used in the ISF's toolset, including the Benchmark and Security Healthcheck.

Material produced by NIST is reviewed as part of input into ISF research projects, involving over 400 international ISF Member organisations. Our key products delivered to ISF Members in the last two years include:

- *new research reports on Security Architecture, Application Security, Managing the Insider Threat, Protecting the Crown Jewels, Aligning Information Risk Management with Operational Risk Management and Preparing for the General Data Protection Regulation*
- *updates to our flagship products – the Standard of Good Practice for Information Security 2016, Benchmark 2016, Information Risk Assessment Methodology 2 (IRAM2) and Threat Horizon 2018 and Threat Horizon 2019*
- *enhanced tools – the Security Healthcheck, Security Radar and IRAM2 Assistant Tool.*

The ISF Standard covers the complete breadth of cyber security, and is divided into 17 categories as shown below.
SG – Security Governance
IR – Information Risk Assessment
SM – Security Management
PM – People Management
IM – Information Management

PA – Physical Asset Management
SD – System Development
BA – Business Application Management
SA – System Access
SY – System Management
NC – Networks and Communications
SC – Supply Chain Management
TS – Technical Security Management
TM – Threat and Incident Management
LC – Local Environment Management
BC – Business Continuity
SI – Security Monitoring and Improvement

Regards
Mark

Mark Chaplin
Information Security Forum
www.securityforum.org